Deutscher Bundestag **Drucksache 17/6971**

17. Wahlperiode 09. 09. 2011

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Agnes Malczak, Omid Nouripour, Tom Koenigs, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 17/6802 –

Cyber-Strategie und Cyber-Außenpolitik der Bundesregierung

Vorbemerkung der Fragesteller

Die „Cyber-Sicherheitsstrategie für Deutschland" der Bundesregierung vom Februar 2011 betrachtet den Schutz des Cyber-Raums als existentielle Frage des 21. Jahrhunderts. Um Sicherheit im Cyber-Raum zu gewährleisten, strebt sie eine enge internationale Zusammenarbeit an, und hebt hierbei insbesondere die NATO (North Atlantic Treaty Organization) hervor. Nach Behördenangaben und Meinung von Expertinnen und Experten hat die Bedrohung des Cyber-Raums in jüngster Zeit zugenommen und mit neuen, insbesondere staatlichen Akteuren eine neue Qualität erreicht. Als eine Antwort eröffnete das Bundesministerium des Innern am 16. Juni 2011 das nationale Cyber-Abwehrzentrum, mit dem künftig schneller auf Angriffe reagiert und das Krisenmanagement optimiert werden soll.

Es gibt berechtigte Zweifel, ob die Strategie der Bundesregierung und das neue Cyber-Abwehrzentrum geeignet sind, die Sicherheit des Cyber-Raums in Deutschland zu verbessern. Es fehlt an technischer Expertise und Ressourcen, um komplexe und gefährliche Angriffe überhaupt zu erkennen und darauf zu reagieren. Auch bezüglich der konkreten Ausgestaltung der internationalen Zusammenarbeit im Cyber-Raum herrscht weitestgehend Unklarheit. Die Beschreibung der Cyber-Außenpolitik der Bundesregierung bleibt vage hinsichtlich Form und Inhalt der von der Bundesregierung angestrebten Abstimmungen, Regulierungen, Kontrollen und Verhaltensnormen sowie der Zuständigkeiten auf internationaler Ebene.

Vor dem Hintergrund der von der Bundesregierung skizzierten Bedrohungslage und angesichts der Aufrüstungsdynamik im Cyber-Raum, fragen wir daher die Bundesregierung.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 7. September 2011 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Grundsätzliche Fragen zur Cyber-Strategie

1. Welche Maßnahmen, Fähigkeiten und Mittel stellt die Bundesregierung bisher konkret zur Prävention und zum Schutz vor Cyber-Angriffen sowie zur Wiederherstellung und zur Reaktion auf derartige Angriffe bereit?

Zu den konkreten bereits laufenden Maßnahmen zählen der Ausbau des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die Zusammenarbeit mit den Trägern der kritischen Infrastrukturen im Rahmen des „Umsetzungsplans KRITIS“, die Intensivierung des Sicherheitsmanagements in der Bundesverwaltung, die Neugestaltung der Netze des Bundes, der Ausbau von Angeboten zur Sensibilisierung wie „BSI für Bürger“, die Einrichtung der Task Force „IT-Sicherheit in der Wirtschaft“ im Bundesministerium für Wirtschaft und Technologie (BMWi) oder die Unterstützung von Initiativen wie „Deutschland sicher im Netz e. V.“ und die Förderung der Anti-Botnetz-Initiative des Verbandes der deutschen Internetwirtschaft e. V. (eco).

Den Polizei- und Justizbehörden des Bundes und der Länder stehen die in den allgemeinen Gesetzen zur Strafverfolgung und Gefahrenabwehr eingeräumten Befugnisse als Reaktion auf Cyber-Angriffe zur Verfügung.

Ziel der von der Bundesregierung im Februar 2011 verabschiedeten Cyber-Sicherheitsstrategie ist, die IT-Systeme in Deutschland sicherer zu gestalten. Hiervon werden sowohl die IT-Systeme der Unternehmen und Behörden als auch die IT-Systeme bei den Bürgern adressiert. Einen besonderen Schwerpunkt bildet die IT im Bereich Kritischer Infrastrukturen.

Um den Informationsaustausch der Sicherheitsbehörden bei Cyber-Angriffen zu verbessern, hat die Bundesregierung zudem im Frühjahr 2011 das Cyber-Abwehrzentrum eingerichtet.

Ende 2011 findet außerdem erstmals eine gemeinsame strategische Krisenmanagementübung zu IT-Vorfällen von Bund, Ländern und Betreibern kritischer Infrastrukturen (LÜKEX 2011) statt.

2. Welche Maßnahmen hat die Bundesregierung ergriffen, um die Bund-Länder-Kooperation im Bereich Cyber-Sicherheit zu verbessern und ein effektives Krisenmanagement im Fall eines Angriffs zu gewährleisten?

Der Bund entwickelt zurzeit mit den Ländern im IT-Planungsrat eine Leitlinie für die Informationssicherheit in der Verwaltung. Durch sie sollen unter anderem Verfahren zur gemeinsamen Abwehr zu IT-Angriffen festgeschrieben werden. Es ist vorgesehen, auch die Zusammenarbeit bei der Bewältigung von IT-Krisen noch konkreter zu regeln.

Die im Fall eines Angriffs ggf. erforderliche polizeiliche Zusammenarbeit zur Krisenbewältigung erfolgt nach dem Vorbild der bewährten Zusammenarbeit in anderen polizeilichen Großlagen. Ende 2011 führen Bund und Länder eine strategische Krisenmanagementübung zu IT-Vorfällen durch (LÜKEX 2011) (vgl. auch Antwort zu Frage 1).

3. Welche Maßnahmen ergreift die Bundesregierung zur Erhöhung des Selbstschutzes gegen Cyber-Angriffe?

   a) Welche Maßnahmen plant sie zur Verbesserung des Meldesystems für den Informationsaustausch?

In § 4 Absatz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) ist die Rolle des BSI als zentrale Meldestelle für die Zu-

sammenarbeit der Bundesbehörden in Angelegenheiten der Sicherheit in der Informationstechnik festgeschrieben. Einzelheiten zur Erfüllung der in § 4 Absatz 3 festgelegten Meldepflicht anderer Bundesbehörden gegenüber BSI sind in einer Allgemeinen Verwaltungsvorschrift aufgrund des § 4 Absatz 6 BSIG geregelt. Im BSI werden zeitnah und zentral alle Informationen zu Cyber-Angriffen gesammelt und ausgewertet, ob ggf. Gefahr für die Bundesverwaltung besteht.

b) Welche Maßnahmen unternimmt sie zur Reduktion der Anzahl von Schnittstellen zwischen Netzen?

Im Projekt „Netze des Bundes“ werden die beiden zentralen ressortübergreifenden Regierungsnetze IVBB und IVBV/BVN in einer leistungsfähigen und sicheren gemeinsamen Netzinfrastruktur neu aufgestellt. Ziel ist es, langfristig eine gemeinsame Infrastruktur für die Bundesverwaltung zu schaffen. Außerdem wird eine Gesamtstrategie für weitere Konsolidierungen von Bundesnetzen und der Bund-Länder-Kommunikation über die Schnittstelle zum Verbindungsnetz DOI in die neue Netzinfrastruktur erarbeitet. Dadurch wird sukzessive die Anzahl der Schnittstellen zum Internet weiter reduziert.

c) Welche Maßnahmen plant sie hinsichtlich der Dezentralisierung und Diversifikation der IT-Systeme (IT = Information Technology)?

„Netze des Bundes“ wird eine leistungsfähige und sichere gemeinsame Netzinfrastruktur für die Bundesverwaltung zur Verfügung stellen, auf deren Basis Behörden ihre Liegenschaften anforderungsgerecht und sicher miteinander vernetzen, behördenübergreifend kommunizieren sowie IT-Verfahren anbieten oder selbst nutzen können.

Bei der Konsolidierung der IT der Bundesverwaltung wird darauf geachtet, auch weiterhin mehrere, geographisch verteilte Rechenzentrum-Standorte zu betreiben. Ebenso wird die Möglichkeit geschaffen, einen sicheren IT-Betrieb für alle Bundesbehörden durch das Angebot entsprechender (Backup-)Rechenzentrumskapazitäten in den IT-Dienstleistungszentren des Bundes zu gewährleisten.

d) Welche Maßnahmen unternimmt sie zum Aufbau von doppelten und mehrfachen Sicherungssystemen (IT-gestützt oder IT-unabhängig) im Bereich kritische Infrastruktur?

Die Bundesregierung passt regelmäßig die Strukturen und Sicherheitsmaßnahmen der IT-Infrastrukturen an die stetig steigende Bedrohung an. Hervorzuheben ist der Kabinettsbeschluss zum Umsetzungsplan Bund aus dem Jahr 2007, der den Weg für ein einheitliches Vorgehen zur Risikobewertung auf Basis der BSI-Standards, den Aufbau von IT-Krisenmanagement und die Weiterentwicklung der regierungsinternen Kommunikationsinfrastrukturen (Netze des Bundes) bereitete.

4. Inwiefern ist nach Ansicht der Bundesregierung eine Trennung von offensiven und defensiven Fähigkeiten im Bereich Cyber-Sicherheit möglich?

   Wie definiert sie in diesem Kontext offensive und defensive Fähigkeiten?

Nach Ansicht der Bundesregierung können offensive und defensive Fähigkeiten im Bereich Cyber-Sicherheit in der Weise voneinander abgegrenzt werden, dass

- defensive Fähigkeiten im Bereich Cyber-Sicherheit vornehmlich präventive Maßnahmen sowie ergänzend responsive Maßnahmen mit Auswirkung ausschließlich im eigenen Herrschaftsbereich umfassen,
- offensive Fähigkeiten danach hingegen solche sind, die Auswirkungen in einem fremden Herrschaftsbereich haben.

5. Hält die Bundesregierung einen digitalen Angriff für einen bewaffneten Angriff im Sinne des Völkerrechts, und wenn ja, wie begründet sie dies?

Die Bundesregierung ist der Auffassung, dass ein Cyber-Angriff nur dann als bewaffneter Angriff im Sinne des Völkerrechts einzuordnen wäre, wenn dieser in seiner Wirkung die Schwelle zum bewaffneten Konflikt überschreiten würde und sich mit derjenigen herkömmlicher Waffen vergleichen ließe. Eine Beurteilung, ob diese Schwelle überschritten wird, setzt eine Bewertung sämtlicher Umstände im Einzelfall voraus.

6. Erfordert der Einsatz von Cyber-Fähigkeiten seitens der Bundeswehr nach Ansicht der Bundesregierung eine Mandatierung durch den Deutschen Bundestag, und wie begründet die Bundesregierung ihre Auffassung?

Die Zustimmung des Deutschen Bundestages ist nach § 1 Absatz 2 des Parlamentsbeteiligungsgesetzes bei jedem Einsatz bewaffneter deutscher Streitkräfte außerhalb des Geltungsbereichs des Grundgesetzes erforderlich. Ausgehend von den in der Cyber-Sicherheitsstrategie für Deutschland beschriebenen Maßnahmen zur Abwehr von Cyber-Angriffen sieht die Bundesregierung keinen Anwendungsfall des Parlamentsbeteiligungsgesetzes.

7. Kann ein Cyber-Angriff vor dem Hintergrund des Rückverfolgungsproblems nach Ansicht der Bundesregierung einen möglichen Fall individueller oder kollektiver Selbstverteidigung im Sinne des Völkerrechts auslösen, und wenn ja, wie begründet sie dies?

Je nach Eigenart erscheint es nicht von vornherein ausgeschlossen, einen Cyber-Angriff im Einzelfall als einen bewaffneten Angriff auf einen Staat zu werten. Dies, insbesondere dann, wenn er sich einem Staat zurechnen lässt, sich der Einsatz gegen die Souveränität eines anderen Staates richtet und sich seine Wirkung mit der Wirkung herkömmlicher Waffen vergleichen lässt. Nur wenn die Wirkung dieses Cyber-Angriffs nach Beurteilung sämtlicher Umstände im Einzelfall die Schwelle zum bewaffneten Angriff überschritte, stünde einem Staat das völkerrechtliche Selbstverteidigungsrecht gemäß Artikel 51 der Charta der Vereinten Nationen zu. Bei Vorliegen der Voraussetzung für eine Bedrohung der internationalen Sicherheit und Ordnung gemäß Artikel 39 der Charta der Vereinten Nationen wären durch den Sicherheitsrat der Vereinten Nationen zu beschließende kollektive Zwangsmaßnahmen denkbar.

Grundsätzliche Fragen zur Cyber-Außenpolitik

8. Welche Form, und welchen Inhalt sollten internationale Regulierungen zur Verbesserung der Sicherheit im Cyber-Raum nach Ansicht der Bundesregierung haben?

In der von der Bundesregierung im Februar 2011 beschlossenen Cyber-Sicherheitsstrategie für Deutschland wurde die Cyber-Außenpolitik als neues Politikfeld definiert, weil Sicherheit, Freiheit und Verfügbarkeit des Internet nur in in-

ternationaler Kooperation gewährleistet werden können. Die Überlegungen der internationalen Gemeinschaft zu Form und Inhalt möglicher internationaler Vereinbarungen stehen noch am Anfang. Die Bundesregierung steht dazu im Dialog mit Wissenschaft, Wirtschaft und der Zivilgesellschaft sowie mit Verbündeten und Partnern im Dialog.

Soweit völkerrechtlich verbindliche Regelungen in Betracht kommen, kann für den Bereich des Strafrechts das Übereinkommen des Europarats über Zusammenarbeit bei der Bekämpfung der Computerkriminalität vom 23. November 2001 (Budapester Konvention) als Leitlinie für internationale Regelungen und deren nationale Umsetzung angesehen werden. Dieses Übereinkommen steht zudem nicht nur den Mitgliedern des Europarats, sondern auch interessierten anderen Staaten auf Einladung des Europarates zum Beitritt offen. Deutschland hat das Übereinkommen am 9. März 2009 ratifiziert.

Demgegenüber erscheint für einen von möglichst vielen Staaten getragenen Kodex für staatliches Verhalten im Cyber-Raum, der als wichtiges Element vertrauens- und sicherheitsbildende Maßnahmen zum Gegenstand haben sollte, zunächst die Entwicklung von konsentierten, nur politisch verbindlichen Verhaltensnormen sinnvoll.

9. Welche Foren und Organisationen auf internationaler Ebene sollten hierbei nach Auffassung der Bundesregierung für jeweils welche Bereiche zuständig sein (bitte insbesondere auf die Vereinten Nationen (VN), die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), die Europäischen Union (EU), der Europarat, die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) oder die NATO eingehen)?

Den Vereinten Nationen kommt die Aufgabe zu, nicht nur zur Sicherheit im Cyber-Raum sondern auch zu wirtschaftlichen und sozialen Aspekten der Informationsgesellschaft gemeinsame Ziele und Maßnahmen zu erarbeiten, die den Interessen aller Länder gleichermaßen gerecht werden. Dazu dient u. a. das Internet Governance Forum (IGF), das als operatives Gremium aus dem von der ITU in zwei Phasen (2003 und 2005) ausgerichteten Weltgipfels zur Informationsgesellschaft (WSIS) hervorgegangen ist. Die Internationale Telekommunikationsunion (ITU) spielt als VN-Agentur eine Rolle bei der Mitwirkung bzw. Schaffung von technischen Voraussetzungen von Cyber-Sicherheit. Im 1. Hauptausschuss der VN-Generalversammlung laufen Arbeiten an möglichen vertrauens- und sicherheitsbildenden Maßnahmen, an denen sich die Bundesregierung aktiv beteiligt (Näheres dazu in der Antwort zu Frage 12).

Der Mehrwert der OSZE liegt aufgrund ihrer langjährigen Erfahrung auf dem Feld der vertrauens- und sicherheitsbildenden Maßnahmen sowie in ihrem Ansatz der mehrdimensionalen Sicherheit. Die Bundesregierung wird sich dafür einsetzen, dass sich diese beiden Aspekte auch in der noch zu erarbeitenden OSZE-Strategie „Cyber-Sicherheit“ wiederfinden.

Die Bundesregierung sieht die Rolle der NATO in erster Linie beim Schutz der eigenen IT-Infrastrukturen und bei der Berücksichtigung von Cybersicherheitsaspekten im militärischen Planungsprozess sowie im „NATO Defence Planning Process“.

Die langfristige Verbesserung von Cybersicherheit durch Maßnahmen kooperativer Sicherheitspolitik, insbesondere durch vertrauensbildende Maßnahmen, Verhaltenskodizes etc. kann durch die NATO in Abstimmung mit anderen internationalen Organisationen unterstützt werden.

Der Europarat hat mit dem o. g. Übereinkommen über Computerkriminalität sowie bei der Zusammenarbeit zur Bekämpfung des Cyber-Terrorismus Maß-

stäbe gesetzt. Laufende verdienstvolle Arbeiten im Rahmen des Europarats betreffen die Meinungs- und Informationsfreiheit im Netz.

Die OECD hat neben Grundsätzen für die IKT-Wirtschaft auch solche für Netzpolitik erarbeitet; damit befasst sich ein eigener Fachausschuss (Committee for Information, Computer and Communications Policy). In diesem Rahmen hat Deutschland im Juni 2011 seine Cyber-Sicherheitsstrategie vorgestellt.

Die Europäische Union (EU) arbeitet an dem Thema Cyber-Sicherheit in einer Vielzahl von Gremien und Initiativen. Als Beispiele seien genannt die ENISA (European Network and Information Security Agency), an deren Stärkung derzeit gearbeitet wird, und die Ratsarbeitsgruppe „Telekommunikation und Informationsgesellschaft“, die sich u. a. mit dem Schutz kritischer Informationsinfrastrukturen“ befasst. Im Bereich des Strafrechts wird derzeit über den Vorschlag der Kommission einer Richtlinie über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates beraten.

10. Welche Position vertritt die Bundesregierung hinsichtlich der verschiedenen möglichen Formen internationaler Kooperationsvereinbarungen?

a) Welche Position vertritt sie hinsichtlich der Schaffung eines Rüstungskontrollregimes für den Cyber-Raum?

Nach dem gegenwärtigen Stand der Meinungsbildung zeichnet sich ab, dass es schwierig wäre, die Mechanismen der traditionellen Rüstungskontrolle unmittelbar auf den Bereich Cyber-Sicherheit zu übertragen, in dem man etwa versuchte, Hard- oder Software quantitativ und qualitativ zu beschränken. Zu groß sind die Definitions- und Verifikationsprobleme, in Bezug auf Cyber-Fähigkeiten kann nur schwer zwischen „zivil“ und „militärisch“ unterschieden werden, und eine eindeutige Zurückverfolgbarkeit von digitalen Angriffen dürfte in der Regel kaum möglich sein. Dennoch lassen die Erfahrungen von im Kontext der Rüstungskontrolle verhandelten vertrauens- und sicherheitsbildenden Maßnahmen hoffen, dass es auch im Cyber-Raum möglich sein wird, zwischen Staaten mit unterschiedlichen Werten und Interessen zu Vereinbarungen zu kommen, um destabilisierende Entwicklungen zu verhindern.

b) Welche Position vertritt sie hinsichtlich der Schaffung verbindlicher Verhaltensnormen und Regeln zum Umgang mit Cyber-Angriffen und gemeinsamen Krisenmanagement?

Ein völkerrechtlich bindendes Übereinkommen, das bei den Beitrittsländern gegebenenfalls umfassenden Rechtsänderungsbedarf auslösen würde, erfordert einen komplexen Verhandlungsprozess und erscheint kurz- bzw. mittelfristig und im großen Rahmen kaum realisierbar. Deshalb rückt als erster Schritt die Entwicklung von politisch verbindlichen Verhaltensnormen in den Blickpunkt. Diese könnten bei Konflikten als Auslegungshilfe herangezogen werden und die Ausbildung von Völkergewohnheitsrecht anstoßen.

c) Welche Position vertritt sie hinsichtlich der Schaffung vertrauensbildender Maßnahmen, insbesondere zur Schaffung von Transparenz?

Die Bundesregierung sieht – wie u. a. in der Antwort zu Frage 10a näher erläutert – die Schaffung vertrauens- und sicherheitsbildender Maßnahmen im Cyber-Raum als vorrangig an und beteiligt sich aktiv an den darauf ausgerichteten Arbeiten. Dabei spielen Maßnahmen zur Förderung der Transparenz zwischen Staaten eine große Rolle.

d) Welche Position vertritt sie hinsichtlich der Schaffung gemeinsamer Fähigkeiten für Cyber-Angriffe mit Partnerländern bzw. im Rahmen von internationalen Organisationen und Bündnissen?

Die Schaffung gemeinsamer Fähigkeiten für Cyber-Angriffe ist nicht beabsichtigt.

11. Welche Initiativen hat die Bundesregierung auf welchen Ebenen, und mit welchen Ergebnissen bisher unternommen, um die internationale Zusammenarbeit zur Verbesserung der Sicherheit im Cyber-Raum voranzutreiben (bitte einzeln auf VN, OSZE, EU, Europarat, OECD und NATO eingehen)?

In den Beratungen der Vereinten Nationen anlässlich des 12. VN-Kongresses zur Verbrechensverhütung und Strafjustiz im April 2010 und den nachfolgenden Sitzungen der VN-Verbrechensverhütungskommission hat die Bundesregierung darauf gedrungen, den bereits bestehenden Regelungen, insbesondere dem Übereinkommen des Europarats über Computerkriminalität, möglichst umfassende Geltung zu verschaffen.

In der EU gestaltet sie Maßnahmen im Rahmen der Strategie der Inneren Sicherheit und der Digitalen Agenda für Europa, die letztlich in eine globale Strategie einzubetten sind, aktiv mit. Im Rahmen dieser Bemühungen kommt der derzeit diskutierten Modernisierung des Mandats für die europäische Agentur ENISA eine besondere Bedeutung zu.

Die Bundesregierung hat das Engagement der NATO im Bereich Cyber-Abwehr begrüßt und aktiv mitgestaltet. Entwicklungsschritte dieses Engagements – bis zum Beschluss der „NATO Cyber Defence Policy“ im Juni 2011 – sind die Etablierung der „NATO Computer Incident Response Capability NCIRC“ (2003), die Aufstellung des „NCIRC Technical Center“ (erste operationelle Fähigkeit 2006), die Verabschiedung der ersten „Cyber Defence Policy“ (2008), die Einrichtung der „NATO Cyber Defence Management Authority“ (2008), die Akkreditierung des „Cooperative Cyber Defence Centre of Excellence (CCD CoE)“ in Tallinn, Estland (2008), die Durchführung von jährlichen Cyber Defence Übungen (seit 2008), die Einrichtung einer Emerging Security Challenges Division mit einer Section Cyber-Defence im NATO Hauptquartier (2010), und die Entwicklung des „NATO Cyber Defence Concept“ (März 2011). Zur OSZE siehe Antwort zu Frage 12.

12. Welche Anstrengungen mit welchen Ergebnissen hat die Bundesregierung bisher unternommen, um einen möglichst universellen Kodex für staatliches Verhalten im Cyber-Raum (Cyber-Kodex) zu etablieren, der auch vertrauens- und sicherheitsbildende Maßnahmen umfasst?

    Welchen Inhalt haben die von der Bundesregierung im Rahmen der Cyber-Sicherheitskonferenz der OSZE im Mai 2011 gemachten Vorschläge der Bundesregierung für einen Verhaltenskodex?

Die Bundesregierung beteiligte sich in den Vereinten Nationen aktiv an der 2005 und erneut 2010 vom 1. Ausschuss der VN-Generalversammlung eingesetzten Regierungsexpertengruppe zu internationalen Aspekten der IT-Sicherheit. 2010 konnte diese Gruppe einen Bericht verabschieden. Damit ist Cyber-Sicherheit zum ersten Mal in einem gemeinsamen Bericht auch zwischen USA, Russland und China im Konsens behandelt worden. Deutschland unterstützt, zusammen mit den USA, die von Russland eingebrachte Resolution der VN-Generalversammlung, die eine weitere VN-Regierungsexpertengruppe zum Thema für 2012 vorsieht.

Im Rahmen dieser Regierungsexpertengruppe wird sich die Bundesregierung für die Schaffung von vertrauens- und sicherheitsbildenden Maßnahmen einsetzen. Vor diesem Hintergrund fördert das Auswärtige Amt ein Projekt mit dem VN-Institut für Abrüstungsforschung (UNIDIR) und dem Institut für Friedensforschung und Sicherheitspolitik (IFSH). Das Projekt untersucht, inwieweit das bestehende Völkerrecht auf den Cyberraum Anwendung finden und konkretisiert werden kann, sowie welche vertrauens- und sicherheitsbildenden Maßnahmen zukünftig sinnvoll erscheinen. Die Forschungsergebnisse werden im Rahmen einer Konferenz im Dezember 2011 mit internationalen Experten und Entscheidungsträgern diskutiert werden.

Die Bundesregierung hat sich bei der Vorbereitung und Durchführung der ersten OSZE-Konferenz zu Fragen der Cyber-Sicherheit im Mai 2011 aktiv beteiligt. Auf der Linie der „Cyber-Sicherheitsstrategie für Deutschland“ schlug die Bundesregierung vor, in den bevorstehenden internationalen Konferenzen zu Fragen der Cyber-Sicherheit dem Aspekt der vertrauens- und sicherheitsbildenden Maßnahmen sowie der Diskussion um mögliche Normen staatlichen Verhaltens im Cyberspace besondere Aufmerksamkeit zu schenken (u. a. Frühwarnung, Transparenz, Entwicklung technischer Empfehlungen, Einrichtung nationaler Focal Points, Aufbau von Kommunikationskanälen für Krisenfälle, Kapazitätsaufbau). Die Konferenz stellte eine wichtige Etappe auf dem Weg zur Ausarbeitung einer OSZE-Strategie „Cyber-Sicherheit“ dar, an der die Bundesregierung auch weiterhin aktiv mitarbeiten wird. Darüber hinaus könnten im OSZE-Rahmen erzielte Ergebnisse möglicherweise Modell für globale Regelungen stehen.

13. Worin liegen nach Auffassung der Bundesregierung die Schwierigkeiten bei der Etablierung eines solchen Kodexes, und durch welche Vorgehensweise versucht sie diese zu beseitigen?

Auf die in der Antwort zu Frage 10a genannten grundsätzlichen, insbesondere definitorischen Probleme wird verwiesen. Zunächst zielen die Bemühungen der Bundesregierung und die befreundeter Regierungen darauf, in einem möglichst großen Kreis von Staaten eine Verständigung auf gemeinsame Prinzipien herbeizuführen.

14. Wie bewertet die Bundesregierung die Empfehlung von Expertinnen und Experten zu einer internationalen Vereinbarung, nach der ein angegriffener Staat unverzüglich und umfassend über den Angriff informieren und infizierte Rechner vom Netz nehmen sollte?

    Auf welcher Ebene sollten solche Vereinbarungen nach Einschätzung der Bundesregierung getroffen werden?

Eine abschließende Bewertung der Empfehlung von Experten liegt nicht vor. Sowohl Nutzen und Chancen als auch Risiken einer solchen transparenten Informationspolitik lassen sich auf Basis heute vorliegender Erkenntnisse nicht in ein allgemeingültiges Verhältnis setzen. Die weitere Beobachtung der globalen Entwicklungen und das Verhalten der Staatengemeinschaft bleiben abzuwarten, bevor internationale Vereinbarungen dazu angestrebt werden sollten. Staatliche Verfügungen, im Einzelfall infizierte Rechner vom Netz zu nehmen, bedürften einer gesetzlichen Grundlage. Dabei könnte die polizeirechtliche Generalklausel zur Gefahrenabwehr in den einzelnen Polizeigesetzen Anwendung finden. Einer solchen Maßnahme müsste jedoch immer eine Abwägung aller damit einhergehenden Folgen (Verhältnismäßigkeitsprüfung) vorangehen.

Unabhängig hiervon haben einzelne Zugangsprovider in ihren Allgemeinen Geschäftsbedingungen sich die Möglichkeit offengehalten, infizierte Rechner vom Netz zu nehmen.

15. Auf welcher Ebene strebt die Bundesregierung internationale Standards für das Krisenmanagement im Fall von Cyber-Angriffen an?

    a) Für welche Aspekte des Krisenmanagements befürwortet die Bundesregierung globale Standards?

    b) Welche konkreten Vorschläge hat die Bundesregierung hierzu, und in welchem Rahmen setzt sie sich dafür ein?

    c) Was hat sie auf Ebene der VN diesbezüglich unternommen?

Die erste EU-weite Cyber-Übung „CyberEurope“ 2010 hat gezeigt, dass ein abgestimmtes Vorgehen für das Krisenmanagement im Fall von Cyber-Störungen hilfreich ist. Eine intensive Zusammenarbeit auf technischer Ebene (CERT) ist anzustreben, eine Verzahnung der Zusammenarbeit auf strategisch-politischer Ebene ein langfristiges Ziel. „Best practices“ sind dafür bereits für bestimmte multilaterale Gremien in Anwendung. Das BSI gestaltet beispielsweise aktuell Kooperationsmechanismen für IT-Lagen innerhalb der EU mit. In einer mittelfristigen Planung ist die Ausweitung von vereinbarten „best practices“ auf andere internationale Partner angedacht. Auf Ebene der VN sind aktuell keine Aktivitäten bezüglich Standardisierung für IT-Krisenmanagement bekannt.

16. Was hat die Bundesregierung bisher unternommen, und welche Maßnahmen plant sie, um die Transparenz im Bereich militärischer und nachrichtendienstlicher Fähigkeiten im Cyber-Raum zu verbessern (bitte insbesondere auf die USA, China, Russland und Großbritannien eingehen)?

Es wird auf die Aussagen zur deutschen Position in der VN/EU/NATO und entsprechenden/weiteren Gremien verwiesen (siehe insbesondere die Antworten zu Frage 10 ff.).

17. Wie bewertet die Bundesregierung die Idee, Frühwarnsysteme in Form automatischer Sensorennetzwerke und Hotlines zwischen Staaten auszubauen?

    Was hat sie in dieser Richtung bisher unternommen, und welche Maßnahmen plant sie?

Das BSI hat gemeinsam mit Hochschulen und Wirtschaftsunternehmen ein datenschutzkonformes IT-Frühwarnsystem auf Basis automatischer Sensorennetzwerke entwickelt. Die gewonnenen Erkenntnisse fließen in das Lagebild des BSI ein.

Das Lagezentrum des BSI steht in engem Kontakt mit anderen Lagezentren von bedeutenden Unternehmen, den SPOC (Single Points of Contact) von Sektoren sowie zu europäischen und internationalen CERTs und Lagezentren von Regierungen.

18. Wie bewertet die Bundesregierung die russische Initiative für einen Rüstungskontrollvertrag für den Cyber-Raum?

Zu den grundsätzlichen Aussichten eines Rüstungskontrollvertrages für den Cyber-Raum wird auf die Antwort zu Frage 10 verwiesen.

a) Welche Konsultationen mit Russland und anderen Staaten fanden hierzu bisher statt, und mit welchen Ergebnissen?

Mit Russland finden regelmäßig Konsultationen statt, u. a. im Rahmen der G8 oder der OSZE sowie bilateral, bei denen auch Fragen der Cyber-Sicherheit und die obigen Vorschläge der Bundesregierung angesprochen werden. In diesem Jahr konnte unter maßgeblicher Mitwirkung der Bundesregierung auf dem G8-Gipfel Einigung darüber erzielt werden, dass die G8-Staaten sich für die Schaffung vertrauens- und sicherheitsbildender Maßnahmen zur Stärkung der Cyber-Sicherheit einsetzen.

b) Welche Schritte plant die Bundesregierung in diese Richtung?

Die Stärkung der Cyber-Sicherheit soll durch die Schaffung vertrauens- und sicherheitsbildender Maßnahmen in mehreren internationalen Foren vorangetrieben werden. Als globaler Ansatz sind hier insbesondere die Vereinten Nationen von besonderer Bedeutung. Die Bundesregierung hat daher die Einrichtung einer neuen VN-Expertengruppe 2012 durch Miteinbringung der entsprechenden russischen Resolution im vergangenen Jahr aktiv unterstützt (siehe Antwort zu Frage 12).

19. Welche Position vertritt die Bundesregierung hinsichtlich der Forderung der VN-Generalversammlung zur Schaffung einer globalen Kultur der Cyber-Sicherheit und zum Schutz kritischer Informationsinfrastrukturen (Resolution 58/199, 30)?

    Was unternimmt die Bundesregierung hierzu auf Ebene der VN?

Die Bundesregierung unterstützt die Resolution 58/199. Sie beteiligt sich daher an der Regierungsexpertengruppe der VN für eine Stärkung der Cyber-Sicherheit.

20. Welche Position vertritt die Bundesregierung hinsichtlich des US-amerikanischen Vorschlags für rechtlich unverbindliche Verhaltensnormen und vertrauensbildende Maßnahmen?

Die Bundesregierung unterstützt diese Herangehensweise und gestaltet den Prozess aktiv mit, wie in der Antwort zu Frage 12 ausgeführt.

21. Was unternimmt die Bundesregierung, um neben euro-atlantischen Institutionen (EU, NATO) auch asiatische und afrikanische Organisationen in die internationalen Abstimmungsprozesse im Bereich Cyber-Sicherheit einzubeziehen (Vereinigung südostasiatischer Staaten zur Förderung von Frieden und Wohlstand – ASEAN, Afrikanische Union)?

Asiatische und afrikanische Staaten sind an den Meinungsbildungen und Arbeiten im Rahmen der VN aktiv beteiligt. Dies unterstreicht z. B. die Abhaltung des nächsten Internet Governance Forum (vgl. Antwort zu Frage 9) im September 2011 in Nairobi. Die Bundesregierung ist im Dialog mit ASEAN/ARF, um künftig Cyber-Sicherheit in geeigneter Weise zu thematisieren. Darüber hinaus wird die Bundesregierung weitere sich bietende Gelegenheiten zu einem Dialog mit den asiatischen und afrikanischen Regionalorganisationen aufgreifen, der nach Auffassung der Bundesregierung über Cyber-Sicherheit hinausgehen und Themen wie Freiheit und Verfügbarkeit des Internet umfassen sollte.

22. Welche Organisationen stehen für die Bundesregierung bei der internationalen Kooperation im Bereich Cyber-Sicherheit im Mittelpunkt?

Auf die Antwort zu Frage 9 wird verwiesen.

Fragen zur Cyber-Außenpolitik im Rahmen der NATO

23. Welche Aufgaben soll die NATO aus Sicht der Bundesregierung hinsichtlich des Themas Cyber-Security übernehmen, wie soll die NATO dies nach Ansicht der Bundesregierung tun, und wie versucht die Bundesregierung, dies im Verbund mit den Partnerländern auf NATO-Ebene umzusetzen?

Bezüglich Cyber-Sicherheit ist es grundsätzliche und vordringliche Aufgabe der NATO, einen effektiven Schutz der bündniseigenen kritischen IT-Infrastruktur zu gewährleisten. Durch die im Juni 2011 von den Verteidigungsministern der Allianz gebilligte „Cyber Defence Policy" werden klare Zuständigkeiten innerhalb der NATO-Strukturen geschaffen mit dem Ziel, robuste Strukturen der „Cyber Defence" aufzubauen, einheitliche Sicherheitsstandards für alle NATO-Netze zu implementieren und gemeinsam mit den zuständigen nationalen Behörden Sicherheitsstandards für nationale Netzwerke, die mit NATO-Netzwerken verbunden sind, zu entwickeln.

Die Bundesregierung hat aktiv an der Entwicklung dieser „Cyber Defence Policy" und des Aktionsplans zu ihrer Umsetzung mitgearbeitet und ihre Vorstellungen eingebracht. Der Aktionsplan wird kontinuierlich weiterentwickelt, die Aufgabenstellung detailliert und operationalisiert und den jeweiligen Gremien und Agenturen der NATO zugewiesen. Auf diese nimmt die Bundesregierung, ebenso wie die Partner, auch weiterhin unmittelbar Einfluss.

24. Welche Position vertritt die Bundesregierung auf NATO-Ebene bezüglich einer Ächtung des Einsatzes von elektronischer Datenverarbeitung und Telekommunikation zur direkten oder flankierenden Kriegsführung?

Die Aufrechterhaltung und Fortentwicklung der Fähigkeit zur vernetzten Operationsführung in einem streitkräftegemeinsamen und multinationalen Verbund verlangt zwingend den breiten Einsatz modernster Mittel der elektronischen Datenverarbeitung und Telekommunikation. Eine Ächtung der Nutzung dieser Mittel ist mithin grundsätzlich weder national noch im Bündnis möglich. Selbstverständlich sind bei jedem Einsatz, auch dem Einsatz von elektronischer Datenverarbeitung und Telekommunikation, die verfassungsrechtlichen Grenzen zu beachten.

25. Welche Eckpunkte enthält die NATO Cyber Defense Policy vom 8. Juni 2011?

    a) Welche Cyber-Sicherheitsmaßnahmen sieht die NATO Cyber Defense Policy vor?

Die überarbeitete und am 8. Juni 2011 beschlossene NATO Policy on Cyber Defence soll insbesondere Cyber-Attacken vorbeugen, die Ausfallsicherheit bzw. die Belastbarkeit der Netze verbessern und auf diese Weise einen wirksamen Schutz der NATO vor Angriffen aus dem Cyber-Raum gewährleisten. Im Zentrum steht die Schaffung klarer Zuständigkeiten für Cyber Defence innerhalb der Organisation mit dem Ziel, einheitliche Grundsätze und Standards für die Netzwerklandschaft der NATO, d. h. NATO-eigene und verbundene Netze durchzusetzen.

b) Welche Grundsätze und Standards sieht die NATO Cyber Defense Policy vor?

Die Strategie sieht eine Kooperation im Bereich Cyber-Abwehr sowohl mit internationalen Organisationen, als auch mit Partnerstaaten vor. Fragen der Cyber-Sicherheit werden im gesamten Aufgabenspektrum der NATO, d. h. sowohl in der Bewusstseinsförderung von Risiken und Bedrohungen im Umgang mit IT bis hin zur Einbeziehung in den militärischen Planungsprozess einschließlich Notfallplanung adressiert, um eine Auftragserfüllung auch bei einer Beeinträchtigung der IT-Netze sicherstellen zu können.

c) Inwiefern enthält die NATO Cyber Defense Policy auch Empfehlungen bzw. Standards für den Austausch von Information über Schwachstellen?

Die Strategie stellt abstrakt klar, dass eine verstärkte internationale Kooperation mit Informationsaustausch zur Analyse von Bedrohungen erforderlich ist und auch Frühwarnmechanismen entwickelt werden sollen.

Die Einzelheiten bleiben einem aus der Strategie abgeleiteten Arbeitsplan überlassen, der die Aufgabenstellungen den jeweils zuständigen Gremien und Agenturen der NATO zuweist.

So wie die Bündnisstaaten maßgeblich an der Formulierung der NATO Policy on Cyber Defence beteiligt waren, werden diese zukünftig auch im Rahmen der Umsetzung unmittelbar Einfluss auf die einzelnen Cyber-Sicherheitsmaßnahmen der NATO über die dafür vorgesehenen Gremien nehmen.

26. Welche unterschiedlichen Ansichten unter den Mitgliedstaaten gibt es bezüglich Strategie und aufzubauenden Fähigkeiten der NATO im Bereich Cyber-Sicherheit?

Sowohl das Cyber Defence Concept als auch die Cyber Defence Policy der NATO sind in den zuständigen NATO-Gremien entwickelt und von den Verteidigungsministern aller Mitgliedstaaten einstimmig gebilligt worden.

27. Welchen konkreten inhaltlichen Beitrag hat die Bundesregierung zur NATO Cyber Defense Policy geleistet?

Die Bundesregierung hat sich während der Erarbeitung der „NATO Cyber Defence Policy“ in den zuständigen Gremien der NATO aktiv und mit Nachdruck für die Verwirklichung ihrer Ziele eingesetzt, durch Vorschläge und Kommentierungen zu den jeweiligen Textfassungen ebenso wie durch intensiven Gedankenaustausch mit anderen Partnern.

Zu den Zielen der Bundesregierung wird auf die Antwort zu Frage 23 verwiesen.

28. Welche Stelle der Bundesregierung hat diesen Beitrag geleistet, und welche Institutionen und Bundesministerien waren involviert?

Die deutschen Interessen im Rahmen der politischen Konsultationen zum Thema Cybersicherheit in der NATO wurden und werden vom in der Bundesregierung federführenden Bundesministerium des Innern (BMI) in enger Abstimmung mit dem Bundesministerium der Verteidigung (BMVg) und dem Auswärtigen Amt (AA) vertreten.

29. Welche Gremien und Agenturen sind für die geplante Ausarbeitung des detaillierten Arbeitsplans zur Umsetzung der NATO Cyber Defense Policy vorgesehen?

Die Ausarbeitung des Aktionsplans zur Umsetzung der „NATO Cyber Defence Policy“ erfolgt unter Aufsicht des „Defence Policy und Planning Committee“ (DPPC) der NATO. An der Umsetzung der einzelnen Arbeitsschritte sind zahlreiche NATO-Gremien und -Agenturen beteiligt; die Ergebnisse werden beim DPPC und beim „Consultation, Command und Control Board“ (C3B) zusammengeführt.

a) Wer nimmt hieran für die Bundesrepublik Deutschland teil, und welche Institutionen und Bundesministerien sind involviert?

An den Sitzungen des DPPC und des C3B zum Thema Cyberabwehr nehmen Angehörige der Deutschen Ständigen Vertretung bei der NATO in Brüssel teil; im für „Information Assurance and Cyber Defence“ zuständigen Unterausschuss des C3B ist die Bundesregierung durch Mitarbeiter des BMVg vertreten. Die Weisungen werden zwischen dem BMI, dem BMVg und dem AA eng abgestimmt.

b) Welche inhaltliche Zielsetzung verfolgt die Bundesregierung hierbei?

Zur inhaltlichen Zielsetzung der Bundesregierung wird auf die Antwort zu Frage 23 verwiesen.

30. Welche Maßnahmen ergreift die Bundesregierung, um bei der Umsetzung der NATO Cyber Defense Policy die Trennung von militärischen und polizeilichen Aufgaben zu wahren?

Die NATO Cyber Defence Policy zielt darauf ab, den Schutz der kritischen Informationstechnologie der NATO durch Maßnahmen der Cyber Defence zu gewährleisten. Aus der Umsetzung dieser politischen Linien ergeben sich keine Konsequenzen für den Vollzug polizeilicher Aufgaben in Deutschland.

31. Welche Positionen vertritt die Bundesregierung hinsichtlich der Befassung der NATO mit der Bekämpfung von Internetkriminalität, wie es das neue strategische Konzept der NATO vorsieht?

Es wird auf die Antwort zu Frage 30 verwiesen.

32. Welchen Beitrag leistet die Bundesregierung im Rahmen ihrer Beteiligung am NATO Cooperative Cyber Centre of Excellence in Tallinn, und mit welchem Personal ist sie dort vertreten?

Das BMVg ist einer der Zeichner des multilateralen „Memorandum of Understanding“, das die Grundlage des von der NATO akkreditierten, nicht aber zur NATO-Kommandostruktur gehörenden „Cooperative Cyber Defence Centre of Excellence“ (CCD CoE) ist. Personell ist die Bundeswehr derzeit mit dem Chef des Stabes, einem wissenschaftlichen Mitarbeiter und einer Rechtsberaterin beteiligt. Entsprechend der Statuten leistet das BMVg einen finanziellen Beitrag zum Budget des CCD CoE in Höhe von derzeit 20 000 Euro je entsandtem Mitarbeiter.

33. Inwiefern hält die Bundesregierung den Aufbau der Cyber Defence Management Authority (CDMA) der NATO für sinnvoll und notwendig?

    a) Welche Aufgaben und Funktionen hat die CDMA derzeit, und wie ist sie personell besetzt (sowohl ziviles als auch militärisches Personal)?

    b) Wie hat die Bundesregierung den Aufbau bisher unterstützt?

    c) Wie beteiligt sich die Bundesregierung derzeit personell und finanziell?

    d) Inwiefern treffen Berichte zu, wonach die CDMA ausgebaut werden soll in „a war-room operation for NATO's cyber defences with actual tactical responses carried out by member states through a ‚coalition of the willing'"[1]?

    e) Inwiefern unterstützt die Bundesregierung eine solche Entwicklung bzw. heißt sie gut?

Mit der im Juni 2011 beschlossenen NATO „Cyber Defence Policy" wurden die Maßnahmen der NATO im Bereich der Cyber Defence organisatorisch neu geordnet. Dabei wurde die CDMA durch das „Cyber Defence Management Board" (CDMB) ersetzt. Dieses Gremium unter Vorsitz des Assistant Secretary General (ASG) for Emerging Security Challenges dient der Koordination der Maßnahmen der einzelnen zivilen und militärischen Organisationseinheiten der NATO im Bereich der Cyber Defence.

Dem CDMB kommt keine ausführende Funktion zu. Vielmehr obliegt dem CDMB auf strategischer Ebene die Verantwortung für die Ausplanung sowie die Entwicklung und Überwachung der Einhaltung von Richtlinien für die NATO Cyber Defence sowie die Koordination von Schutzmaßnahmen im Falle einer konkreten Krise und zur Hilfestellung auf Anfrage eines Mitgliedstaates.

Mitglieder des CDMB sind der ASG for Defence Policy and Planning (DPP), der ASG for Operations, der ASG for Executive Management (EM), der Director General (DG) International Military Staff (IMS)(DG), Chairman C3 Board (ASG DI), der Director NATO HQ C3 Staff (NHQC3), Director NATO Office of Security (NOS), der Director NATO Office of Resources (NOR), SHAPE ACOS J2 and J6, SACT ACOS C4I, der Director NATO CIS Services Agency (NCSA) und der General Manager NATO C3 Agency (NC3A). Zusätzlich eingeladen sind der NATO-Rechtsberater sowie das CCD CoE. Weitere Organisationseinheiten können bei Bedarf hinzugebeten werden. Eine deutsche Beteiligung ist insoweit gegeben, wie diese Funktionen durch deutsches Personal besetzt sind. Die Finanzierung der Arbeit des CDMB erfolgt entsprechend der geltenden Haushaltsregeln aus dem NATO-Budget.

34. Wie bewertet die Bundesregierung das am 10. März 2011 bei einem Treffen der NATO-Verteidigungsminister in Brüssel gebilligte Cyber Defence Concept der NATO?

    Welche Schlussfolgerungen zieht die Bundesregierung für den Aufbau und Vorhalt nationaler, sowohl ziviler als auch militärischer Kapazitäten, die im NATO-Verbund bereitgestellt werden sollen?

Das 2010 beschlossene Strategische Konzept der NATO identifiziert Cyber-Sicherheit als prominente sicherheitspolitische Herausforderung. Die Staats- und Regierungschefs der Allianz haben anlässlich des Gipfeltreffens in Lissabon die Erarbeitung einer neuen NATO Cyber Defence Policy in Auftrag gegeben.

[1] Vgl. Hughes, Rex B.: NATO and Cyber Defence, Atlantisch Perspectief, 2009, Nr.1/8.

Das im März 2011 von den NATO-Verteidigungsministern gebilligte „Cyber Defence Concept“ stellt den ersten Schritt in der Umsetzung des Gipfelauftrags von Lissabon dar. Es bietet den allgemeinen Rahmen, aus dem die im Juni gebilligte Cyber Defence Policy und der Aktionsplan zu ihrer Umsetzung weiterentwickelt wurden.

Sowohl „Cyber Defence Concept“ als auch „Cyber Defence Policy“ belassen die Kontrollbefugnisse für nationale Netze beim jeweiligen Mitgliedstaat. Die Bundesregierung sichert ihre eigenen Netze in eigener Verantwortung und unter Beachtung der bestehenden NATO-Regularien ab. Diese Aufgabe fällt den hierfür zuständigen Behörden und Ämtern des BMI (BSI) und des BMVg (IT-AmtBW) zu. Weder aus dem „NATO Cyber Defence Concept“ noch aus der „NATO Cyber Defence Policy“ ergibt sich zwecks einer Bereitstellung für das Bündnis die Notwendigkeit des Aufbaus zusätzlicher nationaler Kapazitäten.

Fragen zur Cyber-Außenpolitik im Rahmen der EU

35. Was hat die Bundesregierung unternommen, um die vom Wirtschafts- und Sozialrat der Europäischen Union kritisierte Uneinheitlichkeit und mangelnde Koordination innerhalb der EU beim Schutz kritischer Infrastrukturen zu beheben?

Die Aktivitäten zum Schutz Kritischer Informations-Infrastrukturen (CIIP) wurden explizit in der EU erst mit Veröffentlichung eines entsprechenden Aktionsplans in 2009 gestartet. Unter Berücksichtigung dieser doch kurzen Laufzeit sind die Fortschritte im Bereich der Vereinheitlichung und Koordinierung innerhalb der EU beim CIIP beachtlich. Der angedeutete Aktionsplan spannt einen breiten Schirm an Aktivitäten, welche in Summe genau dieses Ziel nachhaltig unterstützten. So sind die aktive Mitarbeit in Expertengremien zum Thema, die aktive Teilnahme bei Vorbereitung und Durchführung von EU-Cyber-Übungen oder die Einbringung von und Vernetzung der deutschen CERT-Kapazitäten nur Beispiele für das Engagement der Bundesregierung in diesem Bereich. In Deutschland erfolgt zum Schutz der kritischen Infrastrukturen von IT-Vorfällen eine enge und koordinierte Zusammenarbeit im Umsetzungsplan KRITIS bereits seit 2007.

36. Welche Initiativen hat sie ergriffen, um die ebenfalls vom Wirtschafts- und Sozialrat angemahnte Transparenz von Sicherheitslücken und -problemen zu verbessern?

Für den Austausch von Sicherheitslücken und -problemen bestehen bereits seit Jahren Strukturen im Rahmen etablierter CERTs sowie der dieser verbindenden Netzwerke – in Deutschland nimmt das BSI dafür eine zentrale Rolle ein. In den internationalen CERT-Netzwerken ist BSI ein kompetenter und sehr aktiver Partner; durch den kontinuierlichen Austausch sowie die verstärkte Vernetzung wird sowohl die Kompetenz in einzelnen Ländern (mit bislang unterwickelten Strukturen) als auch die gemeinsame Koordinierung verbessert. Zudem pflegt das BSI einen vertrauensvollen, engen Austausch sowohl mit den Anbietern entsprechender Produkte als auch mit Anwendern, sofern diese eine besondere Bedeutung haben. Nach § 7 Absatz 1 Satz 1 BSIG kann das BSI zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten und vor Schadprogrammen an die betroffenen Kreise und die Öffentlichkeit weitergeben oder Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen.

37. Was unternimmt die Bundesregierung, um die Europäische Agentur der Informations- und Netzsicherheit, wie von der Europäischen Kommission gefordert, zu stärken?

Die Bundesregierung unterstützt sehr aktiv schon die gegenwärtigen Arbeiten von ENISA; das BSI befindet sich im engen fachlichen Austausch mit ENISA und ist auch im Verwaltungsrat von ENISA vertreten. Im Rahmen der Verhandlungen zur Neumandatierung von ENISA hat die Abstimmung innerhalb der Bundesregierung sowie mit anderen konsultierten Akteuren ergeben, dass für bestimmte Aufgabenbereiche in Zukunft ein Ausbau notwendig sein wird. So bringt die Bundesregierung neben der starken fachlichen Unterstützung die erarbeiteten Notwendigkeiten für ein Nachfolgemandat aktiv in den Verhandlungsprozess ein.

38. Welche Position vertritt die Bundesregierung hinsichtlich der Forderung des Europäischen Parlaments nach einer „Europäische Strategie für Computer- und Netzsicherheit“, und welche Initiativen hat sie in dieser Richtung unternommen?

Da die Bundesregierung erst im Februar 2011 selbst eine Cyber-Sicherheitsstrategie veröffentlicht hat, sieht sie eine derartige Strategie (hier als „Europäische Strategie für Computer- und Netzsicherheit“) natürlich als adäquaten Baustein zur Verbesserung der Cyber-Sicherheit und würde einem entsprechenden Vorhaben der EU-Kommission positiv gegenüberstehen. Die Erfahrungen aus der Erarbeitung auf nationaler Ebene könnten aktiv eingebracht werden – zudem würde so sichergestellt, dass explizit EU-relevante Sachverhalte aufgegriffen und auf EU-Ebene keine Doppelstrukturen zu den nationalen Einrichtungen geschaffen würden.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333